Nova methodus numeros compositos a primis dignoscendi illorumque factores inveniendi.

P. Seelhoff.

Quaeruntur divisores numeri N.

$$\text{Sit } N = w^2 + r$$

atque $N \equiv \rho\,(p)$, ρ significante residuum aliquod quadrati cum ipsius p, numeri primi, ita ut $w_1^2 \equiv \rho\,(p)$ existat.

Sumatur $N = w_1^2 + (w + w_1)(w - w_1) + r$ et designetur $(w + w_1)(w - w_1) + r$ litera b, unde sequitur $b = w^2 + r - w_1^2$.

$$\begin{aligned} \text{At} \qquad w^2 + r &\equiv \rho\,(p) \\ -w_1^2 &\equiv -\rho\,(p) \\ \hline \text{hinc} \qquad b = w^2 + r - w_1^2 &\equiv 0\,(p) \end{aligned}$$

Radix w_1 in $w_1 + py$ amplificata dat

$$N = (w_1 + py)^2 + \{w + (w_1 + py)\}\{w - (w_1 + py)\} + r.$$

Repertis ergo valoribus w, pro numeris primis usque ad 97 circiter, nisi N nimis magnus est (15 figuras non excedens) et pro binariis illorum potestatibus (pro 2, 3, 5 altiores etiam potestates adhibendae sunt), sin autem N major est, modulo congruentiarum pari passu extenso, plures simplices binariae quadratae repraesentationes comparando illos valores evadent et sequentia statui possunt.

Si numerus N compositus est, mox aut duas repraesentationes ejusdem determinantis aut plures adipisceris, e quibus elimininandis communibus factoribus duae ut

$$\begin{aligned} a_1^2 + mc_1^2 &= \mu N \\ \text{et} \quad a_2^2 + mc_2^2 &= \nu N \end{aligned}$$

sequuntur, quae ad dispares radices congruentiae $z^2 \equiv -m\,(N)$ pertinent itaque duos divisores ipsius N producunt.

Sin vero numerus N est primus, haud secus facile ad tales eliminationes pervenies, quae e contrario ad eandem radicem $\pm z$ perducunt. N numerum primum esse pluribus determinantibus unius factoris evadentibus aut ambobus determinantibus $+\Delta$ et $-\Delta$ saepius occurrentibus affirmatur. Certitudinis causa auxilio determinantium repertorum omnes illi numeri primi quorum hi nonresidua sunt quasi inepti ad divisionem excludi possunt.

Variatio quaedam utilis erit, nisi N formam $8n+1$ praebet. Sit *e. g.*, $N = 8n+3$; jam ponatur $N = 3w^2 + r$ et $w_1^2 \equiv \frac{\rho + px}{3}\ (p)$, ita ut aliis numeris primis opus sit. Hoc modo factor 2^n pro b non omittitur.

Habemus similiter atque prius

$$N = 3w_1^2 + 3(w + w_1)(w - w_1) + r.$$

$$\begin{array}{l} \text{At}\ \ 3w^2 + r \equiv \rho\,(p) \\ \quad -3w_1^2 \equiv -(\rho + px) \equiv -\rho\,(p), \text{ unde} \\ \hline b = 3(w + w_1)(w - w_1) + r \equiv 0\,(p). \end{array}$$

Pro calculo ipso ponatur

$$w \mp (w_1 + py) = \alpha, \text{ unde}$$
$$w_1 + py = \pm(w - \alpha) \text{ et}$$
$$w + (w_1 + py) \text{ aut } w - (w_2 + py) = 2w - \alpha$$
$$N = (w - \alpha)^2 + 2(w - \alpha)\alpha + r.$$

Sit praeterea

$$2w \equiv \pm 2\beta\,(p)$$
$$r \equiv \gamma\,(p),$$

tum solvenda est congruentia

$$(\pm 2\beta - \alpha)\alpha \equiv -\gamma\,(p) \text{ sive}$$
$$\alpha^2 \mp 2\beta\alpha \equiv \gamma\,(p) \text{ et ponendo}$$
$$\alpha = \pm\beta + z$$
$$z^2 - (\beta^2 + \gamma) \equiv 0\,(p).$$

Est autem

$$\begin{array}{l} \beta^2 \equiv w^2 \\ \gamma \equiv r \\ \hline \beta^2 + \gamma \equiv w^2 + r \equiv \rho\,(p), \text{ sive ut antea} \end{array}$$
$$z^2 - \rho \equiv 0 \text{ et } z = w_1.$$

Sit, ut ad finem perveniam

$$\beta = \pm(w - py), \text{ habetur atque prius}$$
$$\alpha = w \mp (w_1 + py).$$

Congruentiae igitur et aequationes, quibus tota methodus nititur, hae sunt:

$N = w^2 + r$
$$N \equiv \rho_1(p),\ w_1^2 \equiv \rho_1(p)$$
$$w \equiv \pm\beta_1(p)$$
$$\alpha = \pm\beta_1 + w_1$$

praeterea
$$N \equiv \rho_2(p^2),\ w_2^2 \equiv \rho_2(p^2)$$
$$w \equiv \pm\beta_2(p^2)$$
$$\alpha = \pm\beta_2 + w_2$$

pro 2, 3, 5 denique
$$N \equiv \rho_n(p^n),\ w_n^2 \equiv \rho_n(p^n)$$
$$w \equiv \pm\beta_n(p^n)$$
$$\alpha = \pm\beta_n + w_n$$
$$N = (w-\alpha)^2 + \overset{b}{\overline{(2w-\alpha)\,\alpha + r}}.$$

Si numerus $N = 8n + 3$, etc., ponendum est $N = 3w^2 + \rho$, et loco congruentiarum
$$w_1^2 \equiv \rho_1(p),\ w_2^2 \equiv \rho_2(p^2),\ w_n^2 \equiv \rho_n(p^n)$$
ponendae sunt
$$w_1^2 \equiv \frac{\rho + px}{3}\,(p),\ w_2^2 \equiv \frac{\rho_2 + p^2}{3}\,(p^2),\ w_n^2 \equiv \frac{\rho_n + p^n}{3}\,(p^n) \text{ etc.}$$
et loco $N = (w-\alpha)^2 + (2w-\alpha)\,\alpha + r$ aequatio
$$N = 3\,(w-\alpha)^2 + 3\,\overset{b}{\overline{(2w-\alpha) + r}}$$
ponenda est, etc.; reliqua intacta remanent.

Dentur exempla:

I.
$$N = 7.2^{34} + 1 = 120259084289$$
$$N = 346783^2 + 635200, \text{ unde}$$
$$w = 346783$$
$$N = (346783 - \alpha)^2 + (693566 - \alpha)\,\alpha + 635200$$
$$N \equiv 20\,(31),\ \rho_1 = 20;\ w \equiv +17\,(31),\ \beta_1 \equiv -14$$
$$w_1^2 \equiv 20\,(31),\ w_1 = \pm 12$$
$$\alpha = -14 \pm 12 = 5 \text{ et } 29$$
$$\text{sive}\quad \alpha = 31y + 5,\ 29$$
$$N \equiv 764\,(31^2),\ \rho_2 = 764 \qquad w \equiv +823\,(31^2),\ \beta_2 = -128$$
$$w_2^2 \equiv 764\,(31^2),\ w_2 = \pm 198$$
$$\alpha = -128 \pm 198 = 60 \text{ et } 625$$
$$\text{sive}\quad \alpha = 31^2 y + 60,\ 625.$$

Hoc modo reperitur

$$\begin{array}{l}
\alpha = 2^3y + 0,\ 2,\ 4,\ 6;\ 2^4y + 0,\ 6,\ 8,\ 14;\ 2^5y + 0,\ 14,\ 16,\ 30; \\
\qquad 2^6y + 0,\ 30,\ 32,\ 62;\ 2^7y + 30,\ 32,\ 94,\ 96;\ 2^8y + 30,\ 32,\ 158,\ 160; \\
\qquad 2^9y + 158,\ 160,\ 414,\ 416;\ 2^{10}y + 158,\ 160,\ 670,\ 672.
\end{array}$$

$$\begin{array}{lrlrrl}
\alpha = & 5y + & 0,\ 1; & 5^2y + & 0, & 16;\ 5^3y + 16,\ 50;\ 5^4y + 141,\ 300. \\
\alpha = & 7y + & 2,\ 4; & 7^2y + & 2, & 18. \\
\alpha = & 11y + & 2,\ 3; & 11^2y + & 47, & 68. \\
\alpha = & 19y + & 1,\ 8; & 19^2y + & 115, & 331. \\
\alpha = & 31y + & 5,\ 29; & 31^2y + & 60, & 625. \\
\alpha = & 37y + & 12,\ 26; & 37^2y + & 271, & 581.\ (1369) \\
\alpha = & 47y + & 10,\ 24; & 47^2y + & 762, & 1387.\ (2209) \\
\alpha = & 53y + & 12,\ 49; & 53^2y + & 261, & 2291.\ (2809) \\
\alpha = & 67y + & 2,\ 47; & 67^2y + & 114, & 2146.\ (4489) \\
\alpha = & 71y + & 1,\ 37; & 71^2y + & 3871, & 4119.\ (5041) \\
\alpha = & 97y + & 45,\ 68; & 97^2y + & 1911, & 4798.\ (9409) \\
\alpha = & 127y + & 49,\ 97; & 127^2y + & 1748, & 14400.\ (16129)
\end{array}$$

Habetur

(1) $N = 344833^2 + 2.7.11.2960^2$ (Ex $\alpha = 1950$, $5y + 0$ cum $37^2y + 581$)

(2) $N = 203351^2 + 7.106172^2$ (Ex $\alpha = 143432$, $11y + 3$ cum $127^2y + 14400$)

(3) $N = 350619^2 - 2.11.11026^2$ (Ex $\alpha = -3836$, $11y + 3$ cum $37^2y + 271$)

Ex (1) et (2) sequitur (4) $11.832082029^2 - 2.150479740^2 = 62953059.N$ unde, comparando cum (3),

$$50459950484647^2 - 26380527979530^2 = \mu.N.$$

Maximus communis divisor differentiae $50459950484647 - 26380527979530$ et ipsius N, *i. e.* 317306291 est factor quaesitus, alter est 379.

II. Membrum quadragesimum octavum seriei 0, 1, 1, 2, 3, 5 . . . est

$$N = 2971215073 = 54508^2 + 93009, \text{ et}$$

$$w = 54508$$

$$N = (54508 - \alpha)^2 + \overbrace{(10916 - \alpha)\alpha + 93009}^{b}.$$

Simili modo atque in antecedente exemplo habebitur

$$\begin{array}{lrlr}
\text{pro } 1, & \alpha = 59 & b = & 2.7.17.72^2 \\
2, & \alpha = 4109 & b = & 2.3.7.3204^2 \\
3, & \alpha = -\ 1 & b = & 2.3.23.29.2^2 \\
4, & \alpha = -\ 387 & b = & -\ 3.7.17.344^2
\end{array}$$

5,	$a = -\ 831$	$b = -\ 2.3.23.31.146^2$
6,	$a = -\ 5987$	$b = -\ 2.7.97.712^2$
7,	$a = 93$	$b = 17.29.144^2$
8,	$a = -\ 7519$	$b = -\ 2.31.37.618^2$
9,	$a = -\ 3187$	$b = -\ 2.3.7.31.524^2$
10,	$a = 1517$	$b = 2.7.17.828^2$
11,	$a = 3323$	$b = 3.7.17.992^2$
12,	$a = 3827$	$b = 3.7.29.43.124^2$
13,	$a = -\ 7051$	$b = -\ 7.10812^2$
14,	$a = 15421$	$b = 7.31.37.424^2$
15,	$a = -\ 28707$	$b = -\ 2.7.23.3504^2$
16,	$a = 31143$	$b = 2.3.43.3066^2$
17,	$a = 20561$	$b = 2.17.7314^2$
18,	$a = -\ 5891$	$b = -\ 23.37.43.136^2$
19,	$a = -\ 13573$	$b = -\ 3.7.23.1856^2$
20,	$a = 18305$	$b = 2.3.7.23.73.406^2$
21,	$a = -\ 94257$	$b = -\ 2.3.23.3204^2$
22,	$a = 21801$	$b = 2.3.17802^2$
23,	$a = -\ 24383$	$b = -\ 2.7.23.29.31.106^2$
24,	$a = 19$	$b = 7.556^2$
25,	$a = -\ 99$	$b = -\ 2.3.1336^2$, etc. etc.

(*a*) Ex 15 habemus $83215^2 - 2.7.23.3504^2 = N$
" 19 " $68081^2 - 3.7.23.1856^2 = N$, unde sequitur
$3.4969913^2 - 2.4826470^2 = 9259.N$ et
$1670196456^2 \equiv 6\,(N)$.

Eadem congruentia ex 25

$$54607^2 - 2.3.1336^2 = N$$

derivari potest. Idem attingit in aliis casibus.

(*b*) Perspicuum est, multas repraesentationes atque $x^2 + cy^2 = \mu N$ eliminandis communibus factoribus formari posse, quarum determinans ex uno factore constat.

(*c*) Habentur determinantes $+\ 7\,(13)$ et $-\ 7\,(24)$; $+\ 6\,(25)$ et $-\ 6\,(22)$ etc. Unde concludi potest, numerum N esse primum. Revera auxilio determinantium repertorum cuncti numeri primi usque ad $\sqrt{N}$ quasi inepti ad divisionem excludendi sunt; numerus 2971215073 est igitur numerus primus.

Ut valor ipsius α quam facillime obtineatur, tabulas composui, exhibentes radices congruentiae

$$w_1^2 \equiv \rho_1 (p)$$

pro numeris a 7 usque ad 199, radices congruentiae $w_2^2 \equiv \rho_2 (p^2)$ pro numeris a 7^2 usque ad 47^2, radices congruentiae $w_n^2 \equiv \rho_n (p^n)$ pro 2^3 usque ad 2^{10}, $3'$ usque ad 3^6, $5'$ usque ad 5^4.

Praeterea autem tabulas auxiliares construxi pro modulo p^2 a 53^2 usque ad 199^2.

Nam

$$\rho_2 \equiv \rho_1 (p) \text{ sive } \rho_2 = q.p + \rho_1$$
$$w_1^2 \equiv \rho_1 (p) \text{ sive } w_1^2 = q_0 p + \rho_1$$
$$2\rho_1 u \equiv 1 (p) \text{ et}$$
$$(q - q_0) u \equiv \delta (p)$$

sequitur $w_2 = \pm \delta + w_1$.

Tabulae auxiliares amplectuntur igitur quatuor columnas, quarum inscriptiones sunt

$$\rho_1 \,.\, q_0 \,.\, u \,.\, w_1.$$

BREMEN, Mai 1885.